FORM PTO-1390 (Modified) (REV 11-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)
7156-101XX	10/018944

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/KR00/00640	June 17, 2000 (17.06.00)	June 17, 1999 (17.06.99)

TITLE OF INVENTION
METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY

APPLICANT(S) FOR DO/EO/US
Dongguyn KIM and Jaegug BAE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include itens (5), (6), (9) and (24) indicated below.
4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☒ Certificate of Mailing by Express Mail
23. ☐ Other items or information:

531 Rec'd PCT/P 17 DEC 2001

APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
10/016944	PCT/KR00/00640	7156-101XX

24. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☒	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO	$1040.00
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO	$890.00
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	$740.00
☐	International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4)	$710.00
☐	International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4)	$100.00

ENTER APPROPRIATE BASIC FEE AMOUNT =	$1,040.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	$0.00	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	10 - 20 =	0	x $18.00	$0.00	
Independent claims	1 - 3 =	0	x $84.00	$0.00	
Multiple Dependent Claims **(check if applicable)**.			☐	$0.00	
TOTAL OF ABOVE CALCULATIONS =				$1,040.00	
☐ Applicant claims small entity status. See 37 CFR 1.27). The fees indicated above are reduced by 1/2.				$0.00	
SUBTOTAL =				$1,040.00	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). +				$0.00	
TOTAL NATIONAL FEE =				$1,040.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).** ☐				$0.00	
TOTAL FEES ENCLOSED =				$1,040.00	
				Amount to be: refunded	$
				charged	$

a. ☐ A check in the amount of _____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. **50-0337** in the amount of **$1,040.00** to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **50-0337** A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Robert Berliner, Esq.
Reg. No. 20,121
FULBRIGHT & JAWORSKI L.L.P.
865 South Figueroa Street, 29th Floor
Los Angeles, CA 90017

(213) 892-9200
(213) 680-4518 (fax)

SIGNATURE

ROBERT BERLINER
NAME

Reg. No. 20,121
REGISTRATION NUMBER

December 17, 2001
DATE

#6

PATENT
Atty. Dkt. No.: 7156-101XX/10112637

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Dongguyn KIM, et al.
SERIAL NO.: 10/018,944
FILED: December 17, 2001
FOR: METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY

Examiner: unassigned
Art Unit: unassigned

SECOND PRELIMINARY AMENDMENT

January 15, 2002
FULBRIGHT & JAWORSKI L.L.P.
865 S. Figueroa St., 29TH Floor
Los Angeles, CA 90017-2571

Commissioner of Patents and Trademarks
Washington, DC 20231

Sir:

Preliminary to the examination of the above application, please make the following amendment to the application.

IN THE CLAIMS:

In claim 8, line 1, please delete "2" and insert –3--.

REMARKS

This preliminary amendment is submitted in order to place the claims in

PATENT
Atty. Dkt. No.: 7156-101XX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	Dongguyn KIM, et al.	Examiner:	unassigned
SERIAL NO.:	unassigned	Art Unit:	unassigned
FILED:	December 17, 2001		
FOR:	METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY		

PRELIMINARY AMENDMENT

December 17, 2001
FULBRIGHT & JAWORSKI L.L.P.
865 S. Figueroa St., 29TH Floor
Los Angeles, CA 90017-2571

Commissioner of Patents and Trademarks
Washington, DC 20231

Sir:

Preliminary to the examination of the above application, please make the following amendments to the application.

IN THE CLAIMS:

In claim 4, line 22, please delete "or 3".

In claim 5, line 5, please delete "or 3".

Please add the following new claims:

--7. The method claimed in claim 3, further comprising a step, in case

that there does not exist the step for adding r_t to respective elements to the cc_t or adding r_t, for carrying out a permutation function with respect to the matrix of $cc_{t,(i,j)}$ composed of n matrices between the step for forming $cc_{t,(i,j)}$ and the step for calculating the residue class of M.

8. The method claimed in claim 2, wherein the step for extracting the binary information data includes steps of:

producing inverse matrices w_1^{-1} and w_2^{-1} of the residue class operations with respect to the M of the w_1 and w_2;

producing a matrix s1 according to a following formula by using the inverse matrices:

$$S_1 = \sum_{t=1}^{n} e_t a_t = w_1^{-1} s w_2^{-1}$$

;

calculating a first comparison value from $s_{1,(1,1)}-s_{1,(k1,k2)}$;

obtaining first binary information of (e_1, e_2, ..., e_{11}) from the first comparison value and a super-increasing integer sequence (d_{11}, d_{12}, ..., d_{111});

calculating a vth comparison value from $s_{v,([v/k2]+1,\ v+1-[v/k2]\cdot k1)}-s_{v,(k1,k2)}$ when v has a value of 2 in $w=\sum_{j=1}^{v} l_j$;

obtaining vth binary information of (e_{w+1}, e_{w+2}, ..., e_{w+1v+1}) from the vth comparison value and a super-increasing integer sequence ($d_{v+1,1}$, $d_{v+1,2}$, ..., $d_{v+1,1v+1}$); and

iterating the step for calculating the vth comparison value and the step for obtaining the vth binary information till the v has values from 3 to u.

REMARKS

This preliminary amendment is submitted in order to place the claims in better form for further prosecution. An early action on the merits is awaited.

Respectfully submitted,

Robert Berliner, Esq.
Registration No. 20,121

Telephone: (213) 892-9200
Facsimile: (213) 680-4518

I hereby certify that this correspondence is being deposited as Express Mail EL136021115US in an envelope addressed to: Box Patent Application, Commissioner of Patents and Trademarks, P.O. Box 2327, Arlington, VA 22202 on December 17, 2001.

By _____
Melinda E. Hallmark

METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a method for transmitting binary information through electronic transmission media, and more particularly to a method for encrypting and deciphering binary information in transmission with the use of super-increasing matrix sequence.

Description of the Related Art

In case of transmitting information through electronic transmission media in recent, especially in data transmission between computers, security matter is being gradually amplified. Actually, data transmitted through transmission lines is relatively easily overheard, which means that important information can pass to third party's hands. In order to prevent such risk, it is necessary to encrypt information for transmission not to be easily read by a third party.

For the encryption of information, various types of encryption methods have been proposed. The encryption methods are largely classified into a symmetric-key method and a public key method. The symmetric key method is a method of using a deciphering key identical to an encrypting key, and the public key method is a method of using a deciphering key different from an encrypting key. The symmetric key method has benefits in

one-to-one data transmissions, but has some troublesome problems in multi-to-one data transmissions since different encrypting keys have to be used. The public key method requires a public key open to the public and a private key held by a receiver, so the public key method has an advantage in the multi-to-one data transmissions. That is, if anyone encrypts information to be transmitted by means of the public key, a receiver can deciphers the information with a secret key, that is, a private key the receiver has.

Such public key encryption method has two important elements, which are the safety and efficiency for transmissions. The safety for transmissions is determined according to how difficult a third party who is not the receiver extracts the private key from the public key, and the efficiency for transmissions is determined according to how easily the public key can be produced.

Lots of studies on the public key transmission system have been carried out since a first introduction from Diffie and hellman in 1976, and continue to devise safer system.

The RSA is a public key transmission system devised in 1978 and occupies over 90% of the world market at present. The RSA transmission system employs a mathematical matter in which the prime factorization of integers is difficult as a basic encryption method. However, the RSA transmission system has a drawback in that a lot of time is required in encryption and decryption.

That is, the RSA transmission system delays an information transmission since it takes a long time in generating a cryptographic key, which requires a large capacitor of buffers

in order to lower or control an information transmission rate of a transmitter. In case of requiring the buffers, some actions should be taken in order for information not to be lost when a signal indicating that a receiving station is not ready for receiving the information is generated.

In the meantime, as an alternative for overcoming the problem of the RSA transmission system, a public key transmission system of a knapsack type has been developed. The system is called "knapsack" since it hides the properties of a super-increasing integer sequence in the public key. The super-increasing integer sequence refers to a set of integers $S=(S_1, S_2, \ldots, S_n)$ composed of positive integers satisfying $S_i > \sum_{j=1}^{i-1}$. The system is known to have faster encryption and decryption speeds than the RSA transmission system. Hereinafter, the public key transmission system of the knapsack type will be described in detail.

The public key transmission system of the knapsack type includes steps of: producing a private key and a public key as in the other public key transmission systems, encrypting information with the public key; transmitting the encrypted signal; and deciphering the transmitted encrypted signal with the private key.

With the steps ramified, the private key is first produced and then the public key is produced from the produced private key. Information is encrypted by using the produced public key and then transmitted. A receiver uses the private key to decipher the encrypted information. Such step is described as below with an example.

First of all, a super-increasing integer sequence B is, for example, 12, 17, 33, 74, 316, arbitrarily produced. After that, a larger number M', for example 737, than the sum of the respective numbers of the super-increasing integer sequence is arbitrarily selected. After that, A number W, for example 635, is arbitrarily selected which is smaller than the M' and a prime number against the M' and vice versa. After that, the super-increasing integer sequence B is multiplied by the number W and an residue class operation is carried out based on the M'.

If the result is put as a public key A, the A can be expressed as follows:

A=(W*B)(mod M')

={635*(12, 17, 33, 74, 157, 316)}(mod 737)

=(250, 477, 319, 559, 200, 196)

Through the above step, a private key(B, M', W) and the public key A can be obtained, but it is not easy to produce the private key(B, M', W) from the public key A through a reverse step. The description has been made that the facilitation of the reverse operation becomes a barometer of a public key transmission system.

Now, a description is made on the steps for encrypting information E by the public key A with an example of a binary number 101101.

The information E is encrypted by multiplying the information E by the public key A. That is, if the encrypted information is put as P, the P can be expressed as follows:

P=A • E

=(250, 477, 319, 559, 200, 196) • (1, 0, 1, 1, 0, 1)=1324

So the encryption is accomplished.

If transmitting such encrypted signal, the information prior to the encryption is extracted from the transmitted signal in a receiving stage(deciphering). The step is as follows. That is, the encrypted signal P is multiplied by W^{-1}, wherein the W^{-1} is a positive integer of satisfying $\{W*W^{-1}\}(\text{mod } M')=1$, and then a residue class is obtained based on the M'. If the obtained value is Q, the Q is expressed as follows:

$$Q=(W^{-1}*P)(\text{mod } M')$$
$$=435$$

where, if the P is substituted with A • E, $Q=(W^{-1}*A \bullet E)$, and then if the A is substituted with $(W*B)(\text{mod } M')$, $Q=\{W^{-1}*(W*B)(\text{mod } M') \bullet E\}(\text{mod } M')$.

The W^{-1} is just a constant, so that the W^{-1} can be put in the parentheses. A residue class regarding the M' of the $W^{-1}*W$ is a 1, so that the result expression is $(B \bullet E)(\text{mod } M')$. If the E is defined as $(e_1, e_2, e_3, e_4, e_5, e_6)$, the result expression is re-expressed as follows:

$435=\{(12, 17, 33, 74, 157, 316) \bullet (e_1, e_2, e_3, e_4, e_5, e_6)\}(\text{mod } 737)$. Here, (12, 17, 33, 74, 157, 316) is the super-increasing integer sequence, so that the E can be easily obtained. That is, the information E=(1, 0, 1, 1, 0, 1) prior to the encryption can be easily extracted from $435 = 12e_1 + 17e_2 + 33e_3 + 74e_4 + 157e_5 + 316e_6$.

However, the system is severely affected in its safety by attack methods developed by Brickell, Lagarias, and Odlyzko, Schnor, et al. That is, a private key of a receiver is easily found by a third party, so that a problem information data is easily leaked has occurred. Most of such attach methods rely upon a low density attack method based on the Lattice Basis

Reduction Algorithm. A small number of the public key transmission systems of the knapsack problem so far, including one based on Chor-Rivest, are known to be safe against such attach methods.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a public key transmission system of an improved knapsack type for securing higher safety by increasing transmission efficiency by easily producing an public key and hardly extracting a private key from the public key.

The present invention provides a public key method of the knapsack type using a super-increasing matrix sequence instead of a public key of the knapsack type using a super-increasing integer sequence. The use of a super-increasing matrix sequence in the present invention causes public keys and private keys to be extended to matrix sequences having arbitrary dimensions, which provides a reason on making the extraction of a private key from a public key more difficult. Accordingly, a construction of the present invention is the same as the public key transmission system using the conventional super-increasing integer sequence as stated above, except for producing a super-increasing matrix sequence instead of the super-increasing integer sequence. A description on such construction will be described as follows. That is, the present invention is directed to a binary information auxiliary transmission method comprising, if K_1 and K_2 are positive integers, $k_1 \times k_2$ is an integer larger than 3, and n is an integer larger than 2, steps

of: producing a private key including n matrices composed of $k_1 \times k_2$; producing a public key including n matrices composed of $k_1 \times k_2$ from the private key; dividing binary information to be transmitted into n plural bit sequences $E = \{e_1, e_2, \ldots, e_n\}$, $e_i \in \{0, 1\}$; encrypting the plural bit sequences E by using respective public keys; forming transmission data S by incorporating encrypted information; transmitting the transmission data S to a receiving station; and extracting binary information data from the received transmission data S in the receiving station by using the private key, wherein the step for producing the private key is placed prior to the step for extracting the binary information data.

After producing the public keys, an addition of a random number to respective matrices composing of the public keys and/or the execution of an order change function can make the extraction of a private key from the public key difficult. In the above case, binary information data E to be transmitted can be exactly extracted by adding a certain number and/or executing an inverse function of the order change function before deciphering.

BRIEF DESCRIPTION OF THE DRAWINGS

The above object and other advantages of the present invention will become more apparent by describing the preferred embodiment thereof in more detail with reference to the accompanying drawings, in which:

FIG. 1 is a flow chart for showing a process of producing a private key and a public key according to an embodiment of the

present invention;

FIG. 2 is a flow chart for showing a encryption process by using the public key of FIG. 1; and

FIG. 3 is a flow chart for showing a deciphering process by using the private key of FIG. 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Hereinafter, the present invention will be described in more detail with reference to the accompanying drawings.

FIG. 1 is a flow chart for showing a process of producing a private key and a public key according to an embodiment of the present invention.

The process, first, produces a private key (cc_t, W_1, W_2, M), wherein cc_t indicates n K1×K1 super-increasing matrix sequences, W_1 is a $k_1 \times k_1$ matrix, W_2 is a $k_2 \times k_2$ matrix, which are values corresponding to B, W, and M', respectively, in a public key transmission system of a knapsack based on a super-increasing integer sequence.

First, positive integers k_1, k_2, l_1, l_2, … ,l_u are arbitrarily selected to be $k_1 \times k_2 \geq 3$, $2 \leq u \leq k_1 \times k_2 - 1$, which is referred to as $n = \sum_{s=1}^{u} l_s$ (step 110).

Next, n super-increasing integer sequences having a length l_s with respect to each s($1 \leq s \leq u$) are selected, which is referred to as $d_s = (d_{s,1}, d_{s,2}, \ldots, d_{s,l})$, $1 \leq s \leq u$(step 120). The super-increasing integer sequence means an integer sequence in which $d_{s,j}$ is a positive integer and $\sum_{j=0}^{t} d_{s,j} < d_{s,t+1}, (1 \leq t \leq l_s - 1)$.

After that, a super-increasing matrix sequence having a matrix size of $k_1 \times k_2$ and length n is produced as follows(step 130). If the matrix sequence is referred to as $cc_t = [cc_{t,(i,j)}]$ in $1 \le t \le n$, $1 \le I \le k_1$, $1 \le j \le k_2$, respective $cc_{t,(i,j)}$ are produced as follows.

ⓐ in case of (i,j)=(1,1), $cc_{t(1,1)} = d_{1,t}$ in $1 \le t \le l_1$ and $cc_{t(1,1)}$ has a random positive integer satisfying

$$\sum_{t=l_1+1}^{n} CC_{t,(1,1)} < d_{1,1}$$ in $l_1+1 \le t \le n$.

ⓑ in case that (i,j) satisfies $2 \le (i-1)k_2+j \le u-1$, $cc_{t,(i,j)}$ has a random positive integer in $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$,

$$CC_{t(i,j)} = d_{(i-1)k_2+j,\,t-\sum_{s=2}^{(i-1)k_2+j-1} l_s}$$ in $\sum_{s=1}^{(i-1)k_2+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$,

and another random positive integer satisfying

$$t = \sum_{s=1}^{(i-1)k_2+j} l_s + 1 \;\sim\; n \quad \text{in} \quad \sum_{s=1}^{(i-1)k_2+j} l_s + 1 \le t \le n$$

$$CC_{t,(i,j)} < d_{(i-1)k_2+j,1}$$.

ⓒ in case that (i,j) satisfies $(i-1)k_2+j = u$, $cc_{t(i,j)}$ has a random positive integer in $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$ and

$$CC_{t,(i,j)} = d_{(i-1)k_2+j,\,t-\sum_{s=2}^{(i-1)k_2+j-1} l_s}$$ in $\sum_{s=1}^{(i-1)k_2+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$.

ⓓ in case that (i,j) satisfies $u+1 \le (i-1)k_2+j \le k \times k_2-1$,

$cc_{t(i,j)}$ has a random positive integer in $1 \le t \le n$.

ⓔ (i,j) satisfies $(i-1)k_2+1 = k_1 \times k_2$, $cc_{t(i,j)} = 0$ in $1 \le t \le n$.

After that, an integer M is selected as follows (step 140). That is, a positive integer M satisfying

$$M > Max\left\{ d_{(s,1)} + \sum_{j=1}^{l_s} d_{s,j} \mid S = 1,2,\ldots,u \right\}$$

is randomly selected.

Next, n random positive integers r_1, r_2, …, r_n are selected (step 150).

After that, r_t is added to respective elements of a matrix cc_t and then a matrix(referred to as c_t in Formula 1) selecting a residue class based on the M is produced (step 160).

Formula 1

$$c_{t,(i,j)} \equiv cc_{t,(i,j)} + r_t \pmod{M}$$

After that, a permutation function π with respect to {1, 2, …, n} is selected to produce $b_t = c_{\pi(t)}$ (step 170). Steps 150 and 160 for adding R_t to respective elements or a step 170 for applying the permutation function can be omitted since they are for making the extraction of a private key from public keys difficult.

After that, two matrices W_1 and W_2 having sizes of $k_1 \times k_1$ and $k_2 \times k_2$ respectively are arbitrarily selected to have inverse matrices when performing calculations based on a residue class of M with respect to matrix elements(step 180). Therefore, the private key cc_t(or b_1, b_2, …, b_n), W_1, W_2, M, and π are completed.

Next, a public key is produced from the private key obtained from the above(step 190).

In the step 190, N matrices, a_t,($1 \le t \le n$) are produced

as follows.

Respective elements exist between 0 and M with at ≡ $w_1 b_t w_2 \pmod{M}$. Accordingly, the public key $a_t = (a_1, a_2, \ldots, a_n)$ are completed.

FIG. 2 is a flow chart for showing an encryption process of information to be transmitted by using the public key of FIG. 1.

The encryption is performed by multiplying the information to be transmitted, which is divided into n bits, by the public key(steps 210 and 220).

Let E be the information containing only 0 and 1 and having a length n.

That is, $E = (e_1, e_2, \ldots, e_n)$, $et \in \{0, 1\}$

The encryption is carried out by multiplying information E to be transmitted by a public key a. If an encrypted signal is indicated as S, the S may be expressed as Formula 2 as below:

Formula 2

$$S = \sum_{t=1}^{n} e_t a_t$$

FIG. 3 is a flow chart for showing a deciphering process with respect to an encrypted signal. A process for extracting E from the encrypted signal s is as follows.

W_1^{-1} and W_2^{-1} of residue class operation inverse matrices with respect to M of W_1 and W_2 are calculated and multiplied by s to produce a cyphertext of an intermediate step(steps 310 to 330). Let such result be S_1, then formula 3 is as follows.

Formula 3

$s_1 \equiv w_1^{-1} s w_2^{-1} \pmod{M}$

where, s_1 is a matrix satisfying $0 \leq s_{1,(i,j)} < M$, a formula

$S_1 = \sum_{t=1}^{n} e_t b_t$ is established. The reason the formula $S_1 = \sum_{t=1}^{n} e_t b_t$ is established is because $W_1 W_1^{-1}$ and $W_2 W_2^{-1}$ are 1, respectively.

In the meantime, if $e'_t = e_{\pi^{-1}(t)}$, the following formula is effectuated becase of $e_t = e'_{\pi(t)}$ and $b_t = c_{\pi(t)}$.

$$S_1 = \sum_{t=1}^{n} e_t b_t = \sum_{t=1}^{n} e'_t c_t$$

Next, a value of $(e'_1, e'_2, \ldots, e'_n)$ is obtained as follows by using a configuration of an appropriate equation and a mathematical induction. First, a value of $(e'_1, e'_2, \ldots, e'_{11})$ becomes a solution of $(x_1, x_2, \ldots, x_{11})$ in the equation of

$S_{1,(1,1)} - S_{1,(k_1,k_2)} = \sum_{j=1}^{l_1} x_j d_{1,j}$, and a value of x_j can be easily obtained since $(d_{1,1}, d_{1,2}, \ldots, d_{1,11})$ is a super-increasing integer sequence.

For example, when a value obtained from the calculation of $s_{1,(1,1)} - s_{1,(k1,k2)}$ is "130" and a super-increasing integer sequence is {30, 74, 147}, a solution becomes "0" since "130" is smaller than "147" and a step for comparing "130" with "74" is carried out without any calculation. At this time, the solution is processed as "1" since 130-74 = 56. Lastly, the solution is set to "1" since "56" is larger than "30" when comparing "56" with "30". Accordingly, the desired final solution becomes {1, 1, 0}. This is generally known to those who are skilled in this field.

After that, if a value of $(e'_1, e'_2, \ldots, e'_3)$ is obtained as an assumption of a mathematical induction and $w = l_1 + l_2 + \ldots + l_v$

in $v \in \{1, 2, \ldots, u-1\}$, a value of $(e'_{w+1}, e'_{w+2}, \ldots, e'_{w+lv+1})$ is obtained as follows. That is, the value is obtained from the calculation of the value of $(x_{w+1}, x_{w+2}, \ldots, x_{w+lv+1})$ in an equation of $S_{v,([v/k_2]+1,v+1-[v/k_2]\cdot k_1)} - S_{v,(k_1,k_2)} = \sum_{j=1}^{l_{v+1}} x_{w+j} d_{v+1,j}$ when $S_v = S_1 - \sum_{t=1}^{w} e'_t c_t$. The use of a super-increasing property of $(d_{v+1,1}, d_{v+1,2}, \ldots, d_{v+1,lv+1})$ enables a value of $(e'_{w+1}, e'_{w+2}, \ldots, e'_{w+lv+1})$ to be easily obtained. All the values of $(e'_1, e'_2, \ldots, e'_n)$ are obtained through the mathematical induction method.

After that, the original message of $E = (e_1, e_2, \ldots, e_n)$ is obtained as follows through the use of the property of $e_t = e'_{\pi(t)}$. That is, $E = (e_1, e_2, \ldots, e_n) = (e'_{\pi(1)}, e'_{\pi(2)}, \ldots, e'_{\pi(n)})$ The signal E prior to the encryption is deciphered through the above process.

The public key transmission system based on this method is much better in a speed point of view, compared to the other public key transmission system and shown in Table 1.

Table 1

	Present invention	NTRU	RSA
Operation speed	n	n^2	n^2
Inverse operation speed	n	n^2	n^2
Operation key length	n^2	n	N
Inverse operation key length	n^2	n	N
Message extension degree	1.5-1	3 or 4-1	1-1

As shown in Table 1, the present invention has a much faster speed in the encryption and decryption, compared to the existing NTRU or RSA system. The matter of prolonging a public key length and a private key length does not cause any problem due to the improvement of the performance of system memories

employed at present.

A secure binary information transmission method according to the present invention can overcome the vulnerability with respect to a low density attack method in a public key transmission system of the knapsack type using a super-increasing integer sequence, and also overcome the vulnerability in a speed of an RSA transmission system by rapidly realizing main operations which are additions or comparisons of two numbers in a computer.

Accordingly, the present invention prevents, in case that binary information is transmitted through transmission media, third parties from easy reading as well as accelerates a transmission speed, so it is directly applicable to home banking, electronic commerce business, information exchanges on the internet, and the like.

Although the preferred embodiment of the present invention has been described, it will be understood by those skilled in the art that the present invention should not be limited to the described preferred embodiment, but various changes and modifications can be made within the spirit and scope of the present invention as defined by the appended claims.

CLAIMS

1. In a method for safely transmitting binary information constructed with plural bits through electronic transmission media, the method comprising steps of:

producing a private key including n matrices constructed with $k_1 \times k_2$, when k_1 and k_2 are positive integers, $k_1 \times k_2$ is an integer larger than 3, and n is an integer larger than 2;

producing a public key(matrix sequence a_t) including the n matrices constituted with the $k_1 \times k_2$ from the private key;

dividing the binary information into n plural bit sequences $E = \{e_1, e_2, \ldots, e_n\}$ in $e_i \in \{0, 1\}$;

encrypting the plural bit sequences E respectively by using the public key;

incorporating the encrypted information and forming encrypted transmission data S;

transmitting the encrypted transmission data S; and

extracting the binary information data from the encrypted transmission data S by using the private key.

2. The method as claimed in claim 1, wherein the step for producing the private key includes steps of:

forming u super-increasing integer sequences $d_1, d_2, \ldots, d_u$ expressed as $d_s = (d_{s,1}, d_{s,2}, \ldots, d_{s,1s})$ of a super-increasing integer sequence having a length l_s with respect to each S satisfying a relationship of $1 \leq s \leq u$, after arbitrarily selecting an integer n larger than 2 but less than $k_1 \times k_2 - 1$, selecting u positive integers $l_1, l_2, \ldots, l_u$, and setting the integer n of a total sum of $l_1 + l_2 +, \ldots, +l_u$;

selecting a random integer M larger than

$$Max\left\{d_{(s,1)}+\sum_{j=1}^{l_s} d_{s,j} \mid s=1,2,\ldots,u\right\};$$

forming a matrix w1 having arbitrary $k_1 \times k_1$ elements and a matrix w_2 having $k_2 \times k_2$ elements for which an inverse matrix exists when calculations with respect to respective matrix elements are carried out with a residue class of M;

forming n matrices $cc_{t,(i,j)}$ having $k_1 \times k_2$ by selecting for $cc_{t,(1,1)}$:

1) if (i, j) = (1,1),

a) $d_{1,t}$ in $1 \le t \le l_1$, and

b) a random positive integer of satisfying

$$\sum_{t=l_1+1}^{n} cc_{t,(1,1)} < d_{1,1}$$

in $l_1 \le t \le n$;

2) if (i,j) satisfies $2 \le (i-1)k_2 + 1 \le u-1$,

a) a random positive integer in $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$,

b) $CC_{t,(i,j)} = d_{(i-1)k_1+j,\,t-\sum_{s=1}^{(i-1)k_2+j-1} l_s}$ in

$$\sum_{s=1}^{(i-1)k_2+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$$

, and

c) a random positive integer satisfying

$$\sum_{t=\sum_{s=1}^{(i-1)k_2+j} l_s+1}^{n} cc_{t,(i,j)} < d_{(i-1)k_2+j,1}$$

in $\sum_{s=1}^{(i-1)k_2+j} l_s + 1 \le t \le n$;

3) if (i,j) satisfies $(i-1)k_2 + j = u$,

a) a random positive integer in $1 \le t \le \sum_{s=1}^{(i-1)k_2+j-1} l_s$, and

b) $cc_{t,(i,j)} = d_{(i-1)k_2+j,t-\sum_{s=1}^{(i-1)k_2+j-1} l_s}$ in $\sum_{s=1}^{(i-1)k_2+j-1} l_s + 1 \le t \le \sum_{s=1}^{(i-1)k_2+j} l_s$,

4) if (i,j) satisfies $u + 1 \le (i-1)k_2 + j \le k_1 \times k_2 - 1$, a random positive integer in $1 \le t \le n$, and

5) if (i,j) satisfies $(i-1)k_2 + j = k_1 \times k_2$, "0"; and

calculating a residue class of M as in $c_{t,(i,j)} \equiv cc_{t,(i,j)} \pmod M$, wherein the step for producing the public key is accomplished by producing at satisfying $a_t = w_1\, cc_{t,(i,j)}\, w_2 \pmod M$, the step for forming the encrypted transmission data S is accomplished by producing the S satisfying a formula $S_1 = \sum_{t=1}^{n} e_t a_t$, and the steps for selecting the M and producing the w_1 and w_2 is carried out after the step for forming the super-increasing matrix sequence cc_t and before the step for forming the public key.

3. The method as claimed in claim 2, further comprising a step, after selecting n random positive integers r_1, r_2, ..., r_n, for adding r_t to respective elements between the step for forming the $cc_{t,(i,j)}$ and the step for calculating the residue class of M.

4. The method claimed in claim 2 or 3, further comprising a step, in case that there does not exist the step for adding r_t

to respective elements to the cc_t or adding r_t, for carrying out a permutation function with respect to the matrix of $cc_{t,(i,j)}$ composed of n matrices between the step for forming $cc_{t,(i,j)}$ and the step for calculating the residue class of M.

5. The method claimed in claim 2 or 3, wherein the step for extracting the binary information data includes steps of:

producing inverse matrices w_1^{-1} and w_2^{-1} of the residue class operations with respect to the M of the w_1 and w_2;

producing a matrix s1 according to a following formula by using the inverse matrices:

$$S_1 = \sum_{t=1}^{n} e_t a_t = w_1^{-1} s w_2^{-1}$$

;

calculating a first comparison value from $s_{1,(1,1)}$-$s_{1,(k1,k2)}$;

obtaining first binary information of (e_1, e_2, ..., e_{11}) from the first comparison value and a super-increasing integer sequence {d_{11}, d_{12}, ..., d_{111}};

calculating a vth comparison value from $s_{v,([v/k2]+1,\ v+1-[v/k2]\cdot k1)}$-$s_{v,(k1,k2)}$ when v has a value of 2 in $w = \sum_{j=1}^{v} l_j$;

obtaining vth binary information of (e_{w+1}, e_{w+2}, ..., e_{w+1v+1}) from the vth comparison value and a super-increasing integer sequence ($d_{v+1,1}$, $d_{v+1,2}$, ..., $d_{v+1,1v+1}$); and

iterating the step for calculating the vth comparison value and the step for obtaining the vth binary information till the v has values from 3 to u.

6. The method as claimed in claim 4, wherein the step for extracting the binary information data includes steps of:

forming inverse matrices W_1^{-1} and w_2^{-1} with the residue class of M of w_1 and w_2;

forming a matrix s_1 according to a following formula by using the inverse matrices:

$$S_1 = \sum_{t=1}^{n} e_t a_t = w_1^{-1} s w_2^{-1}$$

, wherein e_i is a function of "0" and "1" and b_t is a matrix of $k_1 \times k_2$;

calculating a first comparison value from $s_{1,(1,1)}-s_{1,(k1,k2)}$;

obtaining first binary information of (e_1, e_2, ..., e_{11}) from the first comparison value and a super-increasing integer sequence {d_{11}, d_{12}, ..., d_{111}};

calculating a vth comparison value from $s_{v,([v/k2]+1,\ v+1-[v/k2]\cdot k2)}-s_{v,(k1,k2)}$ when the v has a value of 2 and $w = \sum_{j=1}^{v} l_j$;

obtaining vth binary information of (e_{w+1}, e_{w+2}, ..., e_{w+1v+1}) from the vth comparison value and a super-increasing integer sequence ($d_{v+1,1}$, $d_{v+1,2}$, ..., $d_{v+1,1v+1}$);

iterating the step for calculating the vth comparison value and the step for obtaining the vth binary information till the v has values from 3 to u; and

applying an inverse function of the permutation function) to the (e_1, e_2, ..., e_{1u}).

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 December 2000 (28.12.2000)

PCT

(10) International Publication Number
WO 00/79692 A1

(51) International Patent Classification[7]: H04B 1/00

(21) International Application Number: PCT/KR00/00640

(22) International Filing Date: 17 June 2000 (17.06.2000)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
99/22638 17 June 1999 (17.06.1999) KR

(71) Applicant and
(72) Inventor: KIM, Donggyun [KR/KR]; Korea University, Anam-dong 5-1, Seongbuk-gu, Seoul 136-701 (KR).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BAE, Jaegug [KR/KR]; Dongsam-1dong, Youngdo-gu, Pusan 606-081 (KR).

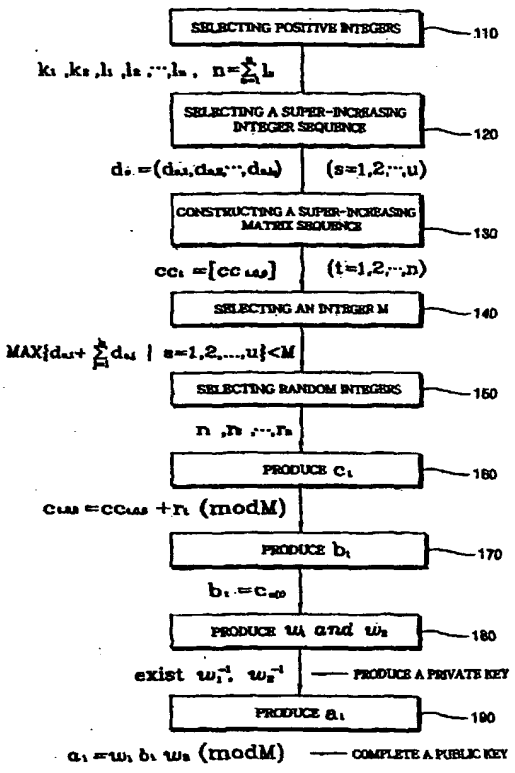
(74) Agents: PARK, Hae-sun et al.; Yoksam-dong 824-19, Gangnam-gu, Seoul 135-080 (KR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY



(57) Abstract: The present invention relates to a method for transmitting binary information through electronic transmission media, which comprises a step of producing a public key and a private key as a preparatory stage for encrypting binary information data, a step of encrypting binary information by using the public key, and a deciphering step wherein super-increasing matrix sequences are used in producing the public key and the private key for encryption.

WO 00/79692 A1

FIG.1

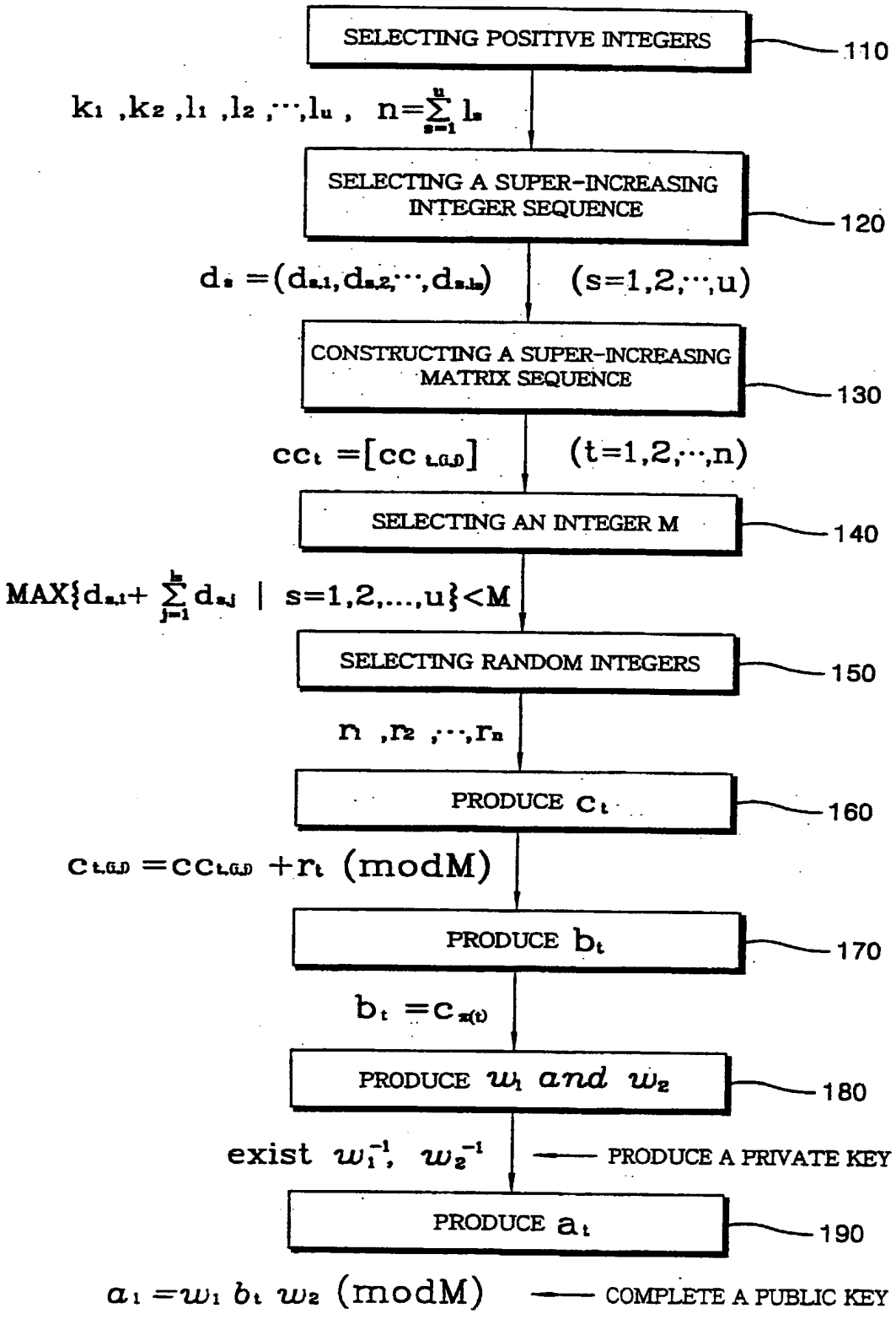

SELECTING POSITIVE INTEGERS
110
$k_1, k_2, l_1, l_2, \cdots, l_u, \quad n=\sum_{s=1}^{u} l_s$
SELECTING A SUPER-INCREASING INTEGER SEQUENCE
120
$d_s=(d_{s,1}, d_{s,2}, \cdots, d_{s,l_s}) \quad (s=1,2,\cdots,u)$
CONSTRUCTING A SUPER-INCREASING MATRIX SEQUENCE
130
$cc_t=[cc_{t,G,D}] \quad (t=1,2,\cdots,n)$
SELECTING AN INTEGER M
140
$MAX\{d_{s,1}+\sum_{j=1}^{l_s} d_{s,j} \mid s=1,2,\ldots,u\}<M$
SELECTING RANDOM INTEGERS
150
$r_1, r_2, \cdots, r_n$
PRODUCE c_t
160
$c_{t,G,D}=cc_{t,G,D}+r_t \pmod{M}$
PRODUCE b_t
170
$b_t=c_{\pi(t)}$
PRODUCE w_1 and w_2
180
exist w_1^{-1}, w_2^{-1}
PRODUCE A PRIVATE KEY
PRODUCE a_t
190
$a_i=w_1 b_t w_2 \pmod{M}$
COMPLETE A PUBLIC KEY

FIG.2

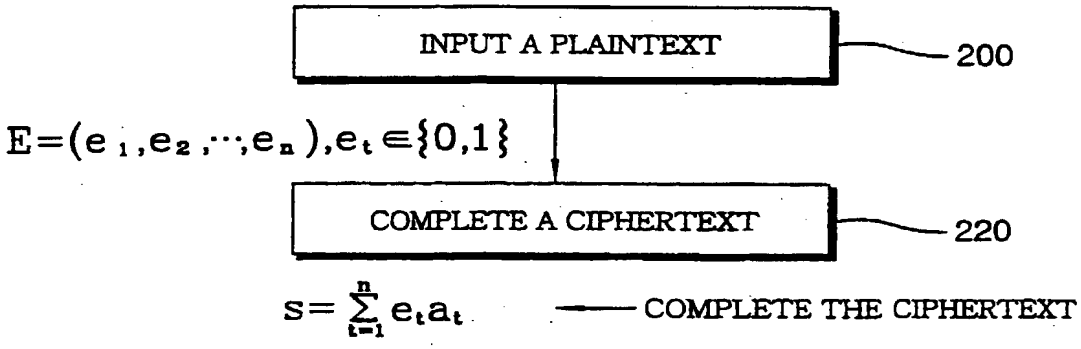
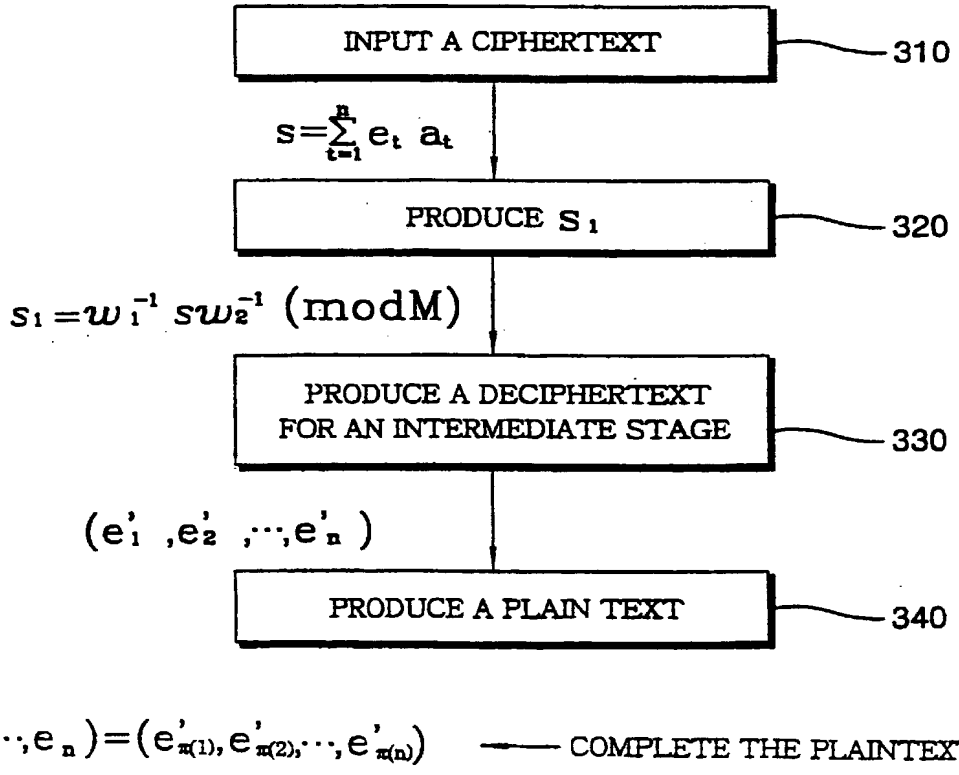


FIG.3



$E=(e_1,e_2,\cdots,e_n)=(e'_{\pi(1)},e'_{\pi(2)},\cdots,e'_{\pi(n)})$ —— COMPLETE THE PLAINTEXT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD FOR TRANSMITTING BINARY INFORMATION WITH SECURITY

the specification of which was filed on December 17, 2001 as Application No. 10/018,944.

In the event that the filing date and/or Application No. are not entered above at the time I execute this document, and if such information is deemed necessary, I hereby authorize and request my attorneys/agent(s) at **Fulbright & Jaworski L.L.P.**, 865 South Figueroa, Twenty-Ninth Floor, Los Angeles, California 90017-2571, to insert above the filing date and/or Application No. of said application.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to herein.

I acknowledge the duty to disclose all information known to me that is material to patentability in accordance with Title 37, Code of Federal Regulations, § 1.56.

FOREIGN PRIORITY CLAIM

I hereby claim foreign priority benefits under Title 35, United States Code §·119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

☐ no such foreign applications have been filed

☒ such foreign application have been filed as follows:

Declaration for Patent Application
I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail, in an envelope addressed to: Commissioner for Patents, Washington, DC 20231, on the date shown below.

Dated: 7/30/02 Signature: _____ (Melinda E. Hallmark)

EARLIEST FOREIGN APPLICATION(S), IF ANY FILED WITHIN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION

Application Number	Country	Date of Filing	Priority Claimed Under 35 USC 119
			___ Yes No ___
			___ Yes No ___
			___ Yes No ___

ALL FOREIGN APPLICATION(S), IF ANY FILED MORE THAN 12 MONTHS (6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION

Application Number	Country	Date of Filing
99/22638	KR	June 17, 1999

CLAIM FOR BENEFIT OF EARLIER U.S. PROVISIONAL APPLICATIONS

I hereby claim priority benefits under Title 35, United States Code §119(e), of any United States provisional patent application(s) listed below:

[x] no such U.S. provisional applications have been filed.

[ ] such U.S. provisional application have been filed as follows:

Application Number	Date of Filing	Priority Claimed Under 35 USC 119
		___ Yes No ___
		___ Yes No ___
		___ Yes No ___

CLAIM FOR BENEFIT OF EARLIER U.S./PCT APPLICATION(S)

I hereby claim the benefit under Title 35, United States Code, §120 of the United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose all information that is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56 which became available to me between the filing date of the prior application and the national or PCT international filing date of this application:

☐ no such U.S./PCT applications have been filed.

☒ such U.S./PCT application have been filed as follows:

Application Number	Date of Filing	Status (Patented/Pending/Abandoned)
PCT/KR00/00640	June 17, 2000	pending

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint:

Robert Berliner	20,121	John M. May	26,200	Terri L. Sale	45,066
M. John Carson	25,090	Billy Robbins	18,313	Miles Yamanaka	45,665
Margaret A. Churchill	39,944	Greg B. Wood	28,133		

all of **Fulbright & Jaworski L.L.P.**, 865 South Figueroa, Twenty-Ninth Floor, Los Angeles, California 90017-2571, jointly, and each of them severally, my attorneys at law/patent agent(s), with full power of substitution, delegation and revocation, to prosecute this application, to make alterations and amendments therein, to receive the patent, and to transact all business in the U. S. Patent and Trademark Office connected therewith.

Please mail all correspondence to Robert Berliner, whose address is:

Fulbright & Jaworski L.L.P.
865 South Figueroa
Twenty-Ninth Floor
Los Angeles, California 90017-2571

Please direct telephone calls to: Robert Berliner at (213) 892-9237.

Please direct facsimiles to: (213) 680-4518

Full name of sole or first inventor
Dongguyn Kim
Sole or first inventor's signature: Dongguyn Kim — Date: July 12, 2002
Residence: Seoul 136-701, Korea, Republic of KR
Citizenship: KR
Mailing Address: Korea University, Anam-dong 5,1 Seongbuk-gu Seoul 136-701 KOREA, REPUBLIC OF

Full name of second inventor, if any
Jaegug Bae
Second inventor's signature: Jaegug Bae — Date: July 12, 2002
Residence: Pusan 606-081, Korea, Republic of KR
Citizenship: KR
Mailing Address: Dongsam-Idong, Youngdo-gu Pusan 606-081 KOREA, REPUBLIC OF

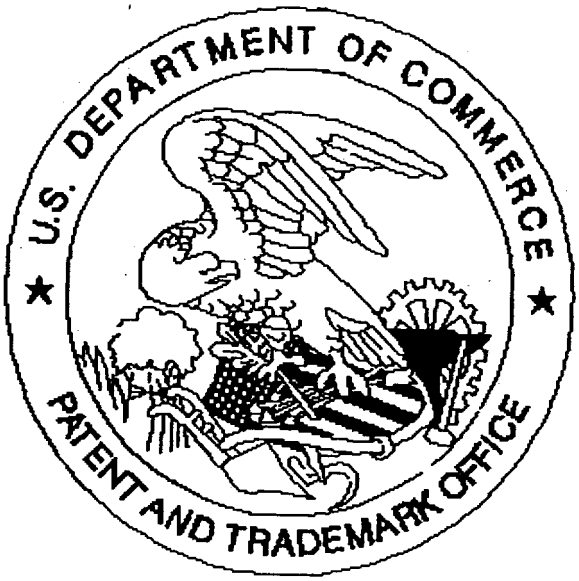
Full name of third inventor, if any	
Third inventor's signature	Date
Residence	
Citizenship	
Mailing Address	

Full name of fourth inventor, if any	
Fourth inventor's signature	Date
Residence	
Citizenship	
Mailing Address	

SCANNED,# 10

United States Patent & Trademark Office

Office of Initial Patent Examination -- Scanning Division



Application deficiencies found during scanning:

☒ Page(s)_____ of Certificate mail were not present for scanning.
(Document title)

☐ Page(s)_____ of _____ were not present for scanning.
(Document title)

☐ ***Scanned copy is best available.***